REMARKS

Summary of Office Action

Claims 1-13 were pending.

Claims 1-13 have been rejected under 35 U.S.C. § 103(a) as being obvious from Franklin et al. U.S. patent No. 6,000,832 ("Franklin") in further view of Rosen U.S. patent No. 6,205,436 ("Rosen").

Applicants' Reply

Applicants have amended claims 1-13 for clarity, and further present new claims 14-17 for examination. Applicants respectfully traverse the prior art rejections.

Applicants' invention relates to systems and methods for authorizing on-line payment transactions between a merchant and a customer, in a manner in which the customer's payment account number is secured by encryption. The payment account number is encrypted in manner, which preserves payment account number privacy, but allows the proper customer payment account to used for routing the payment authorization request from the merchant to the proper bank (e.g., customer's payment card issuer) for authorization and conversely allows the banks response to be routed to the proper merchant.

Claims 1 and 5

The inventive methods, according to claims 1 and 5, involve a service provider (e.g., MasterCard) to mediate the flow of authorization requests and responses. A merchant transaction authorization request is routed (e.g., via a first acquirer) to a service provider identified in the request by a service provider identification number. The service provider processes and routes the authorization request (e.g., via a second acquirer) to an issuer identified in the request (by an issuer identification number). The authorization requests do not explicitly include the customer's payment account number (i.e. unencrypted versions thereof). Unencrypted versions of the customer's payment account number are accessible only to the issuer but not to the service providers, acquirers or other parties on the computer network. Conversely, the issuer's response is propagated back to the transacting parties via the service provider and the first and second acquirers, who are identified by appropriate codes in the response.

Applicants respectfully submit that the methods of claims 1 and 5 are not shown by Franklin and Rosen.

Franklin, as correctly noted by the Examiner, relates to the use of a "digital" card that can be used by a customer for online commerce over a public network. Franklin describes a temporary transaction number in which a code number replaces four digits designated for the customer account number in the 16 digits of a regular credit card number. The customer provides the temporary transaction number to the merchant as a proxy for a regular or conventional card number. The transaction number includes conventional "issuer identification" digits, which the merchant uses to submit the transaction number for approval over the public network to the issuing institution. The issuing institution recognizes the transaction number as a proxy and retrieves the regular card number for processing. (See Franklin, Abstract, Summary of Invention, col. 2 line 1- col. 3 line 24, and FIGS. 1-7).

Further, the Examiner correctly notes that Franklin mentions a conventional "acquiring bank" which forwards merchants requests to the issuing bank. (Franklin See col. 11 lines 38-45). However, applicants note that Franklin's method unlike applicants methods, does not involve the use of a service provider to mediate the transaction between the merchant and the issuer. (See e.g. Franklin FIGS. 1 and 7). In particular, Franklin does not describe "a service provider identification number associated with the service provider other than the payment account issuer" or receipt of the transaction number by the so-identified a service provider, which are required by claims 1 and 5.

The second cited reference – Rosen, relates to a system for electronic commerce in which trusted agents/modules operate as proxies on behalf of customers and merchants. (See e.g., Rosen, Abstract, and FIGS. 1 and 13). Rosen provides the customer and merchant trusted agents (e.g., customer agent A and merchant agent B) with respective "trusted agent/money modules." For purchases of electronic merchandise, an encrypted communication session is established between trusted agent A and trusted agent B. (See e.g., FIGS. 12A, 12 B, 13, 14 and 15, and col. 17 line 54- col. 18 line 65). Payment of merchandise transactions between the customer and merchant can be made anonymously (e.g., using respective money modules) by encrypted, but direct, communications between trusted agent A and trusted agent B. (See e.g., col. 19 line 52- col. 20 line 15).

Rosen's method does not involve the use of a service provider to mediate the transaction between the merchant and the issuer. In particular, like Franklin, Rosen does not describe a service provider identification number associated with "the service provider other than the payment account issuer" or receipt of the transaction number by the so-identified a service provider, which are required by claims 1 and 5.

For at least this reason, claims 1 and 5 are patentable over Franklin and Rosen even when the two references are viewed together.

Claims 9, 14 and 17

Claim 9 and new claims 14 and 17 describe additional features of applicants' method for secure payment transactions. In particular, these claims require computer generation of a message or transaction authentication code, which is positioned in the discretionary data field of a standard payment card track image and then transmitted over the electronic payment network.

Applicants respectfully submit that neither Franklin nor Rosen show this feature of claim 9. Rosen does not describe any standard payment card track image. Franklin's customer computer embeds a code number in the reserved digits of the customer account number (e.g., a standard 16 digit credit card number) to create a temporary transaction number. (See e.g., Franklin FIG. 5). However, Franklin does not show, teach or suggest directly positioning and transmitting the computer generated transaction/message authentication code in the discretionary data field of a standard payment card track image . . . over the electronic payment network.

For at least this reason, claims 9, 14 and 17 are patentable over the cited references.

Dependent claims 2-8, 10-13 and 15-16

Dependent claims 2-8, 10-13 and 15-16 are patentable over the cited references for at least the same reasons discussed above in context of their parent claims 1, 9 and 14, respectively.

Conclusion

In view of the foregoing remarks, favorable consideration and allowance of claims 1-17 are respectfully solicited. In the event that the application is not deemed in condition for allowance, the Examiner is requested to contact the undersigned in an effort to advance the prosecution of this application.

Respectfully submitted,

BAKER BOTTS L.L.P.

Dated: February 15, 2006

Robert C. Scheinfeld
Patent Office Reg. No. 31,300

BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112-4498
Attorney for Applicants
212-408-2500